Baustellen im polizeilichen Datenschutz – Zur Umsetzung der JIRL in den Ländern

Gastautor 2019-03-19T10:00:48

von SEBASTIAN GOLLA und ANNA MICHEL

Der polizeiliche Datenschutz befindet sich im Umbruch. Ein Grund hierfür ist die Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (Richtlinie Justiz und Inneres, im Folgenden: JIRL). Neben der gleichzeitig verabschiedeten Verordnung (EU) 2016/679 (DSGVO) ist die JIRL der weniger beachtete Part der europäischen Datenschutzreform. Während die DSGVO die Verarbeitung von personenbezogenen Daten durch den Staat und Private im Allgemeinen regelt, umfasst die JIRL unter anderem die polizeiliche Datenverarbeitung zu präventiven und repressiven Zwecken. Dieser Beitrag wirft einen genaueren Blick auf die Umsetzung der JIRL in den Polizei- und Datenschutzgesetzen der Länder.

Die Umsetzung der JIRL

Die JIRL war zum 6. Mai 2018 umzusetzen. Allerdings haben bis jetzt nur etwa die Hälfte aller Bundesländer die Umsetzung aus ihrer Sicht vollständig abgeschlossen (Bayern, Berlin, Hessen, NRW, Rheinland-Pfalz, Schleswig-Holstein und Thüringen). Aus manchen Ländern sind hingegen noch keinerlei konkrete Entwürfe zur Umsetzung der JIRL (öffentlich) bekannt (Bremen und Saarland). Soweit die Umsetzung bereits erfolgt oder konkret angegangen ist, lassen sich unterschiedliche gesetzgeberische Ansätze nachvollziehen. Einige Länder haben die Umsetzung der

JIRL zunächst in den allgemeinen Datenschutzgesetzen geplant bzw. vollzogen. Andere Länder nehmen die Umsetzung über spezielle Fachgesetze bzw. eigene „JIRL-Gesetze“ in Angriff.

Wir besichtigen im Folgenden drei zentrale Baustellen bei der Umsetzung der JIRL, die in mehreren Ländern Schwierigkeiten bereiteten: die Einwilligung als Verarbeitungsgrund, Ausnahmen von Betroffenenrechten und die Aufsichtsbefugnisse der Landesdatenschutzbeauftragten.

Einwilligungen mit Beigeschmack

Viele Gesetze zur Umsetzung der JIRL gehen davon aus, dass polizeiliche Datenverarbeitungen zulässig sind, wenn der/die Betroffene eingewilligt hat. Dabei ist diese Konstruktion äußerst heikel. Aufgrund des strukturellen Machtungleichgewichts zwischen Polizei und Bürgern wird eine freiwillige Einwilligung nur selten möglich sein. Auch die JIRL nennt die Einwilligung in ihrem verfügenden Teil nicht als Erlaubnistatbestand zur Datenverarbeitung. Nur aus ErwGr 35 und 37 JIRL ergibt sich, dass eine Einwilligung in Ausnahmefällen und bei einer ausdrücklichen Rechtsgrundlage möglich ist.

Im Anwendungsbereich der JIRL lässt sich daher nicht allgemein regeln, dass eine Datenverarbeitung durch die Polizei zulässig ist, wenn die betroffene Person eingewilligt hat. Zum Teil finden sich in den Gesetzen zur Umsetzung der JIRL bzw. entsprechenden Entwürfen jedoch solche Regelungen – so z.B. in § 9 Abs. 1 Nr. 2 PolG NRW und Art. 28 Abs. 2 Nr. 2 BayDSG i.V.m. Art. 6 Abs. 1 lit. a DSGVO. Diese Vorschriften sind nicht spezifisch genug, sichern die Freiwilligkeit der Einwilligung nicht ab und genügen den Anforderungen der JIRL damit nicht.

Aufgeweichte Betroffenenrechte

Weitere Probleme bestehen bei der Umsetzung der Betroffenenrechte. Die JIRL sieht weitgehende Rechte vor, über Datenverarbeitungsvorgänge informiert zu werden sowie auf diese einwirken zu dürfen. Sie erlaubt Ausnahmen davon unter anderem, wenn dies zur Gewährleistung ungehinderter behördlicher Ermittlungen und Verfahren oder zum Schutz der öffentlichen oder nationalen Sicherheit notwendig ist. Die Landesgesetze zur Umsetzung der JIRL schießen über den Rahmen dieser zulässigen Ausnahmen hinaus.

Dies gilt etwa für Ausnahmen von dem Recht auf Löschung personenbezogener Daten. So sieht etwa § 14 Abs. 2 Satz 2 SächsDSUG-E vor, von einer verlangten Löschung abzusehen, „wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden“. Art. 16 Abs. 3 JIRL beschränkt die Möglichkeit, eine Einschränkung der Verarbeitung statt einer Löschung vorzusehen, im Wesentlichen auf die Fälle, dass die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet und die Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann (Art. 16 Abs. 3 lit. a JIRL) sowie dass die personenbezogenen Daten für Beweiszwecke weiter aufbewahrt werden müssen (Art. 16 Abs. 3 lit. b JIRL). Das bedeutet, dass sich die in § 14 Abs. 2 Satz 2

SächsDSUG-E vorgesehene Ausnahme in der JIRL nicht wiederfindet und die JIRL damit fehlerhaft umgesetzt wurde.

Ebenfalls nicht von der JIRL gedeckt sind Regelungen, die es aufgrund eines „unverhältnismäßigen Aufwandes“ erlauben, von der Löschung abzusehen – so etwa § 44 Abs. 3 Satz 1 Nr. 3 Satz 3 Nr. 3 BlnDSG, § 53 Abs. 3 Satz 1 Nr. 3 HDSIG und § 34 Abs. 3 Nr. 3 LDSG Schleswig-Holstein. Art. 16 Abs. 3 JIRL ist als abschließend zu verstehen, so dass ein ökonomischer oder administrativer Aufwand nicht vorgebracht werden kann, um das Löschungsrecht einzuschränken.

Zahnlose Datenschutzaufsicht

Schließlich enthalten mehrere Landesregelungen zur Umsetzung der JIRL keine ausreichenden Befugnisse für die Datenschutzaufsicht. Die Landesbeauftragten für den Datenschutz sind die wichtigsten Akteure, wenn es um die Durchsetzung des Datenschutzrechts geht. Nach Art. 47 Abs. 2 JIRL sind sie mit wirksamen Abhilfebefugnissen auszustatten – z.B. um Datenverarbeiter verwarnen (lit. a) oder Verarbeitungsvorgänge einschränken und verbieten (lit. b und c) zu können. Das Gebot der Wirksamkeit erfordert dabei zumindest minimale Befugnisse zu einer verbindlichen Einwirkung auf Datenverarbeitungen.

Die Landesgesetzgeber beherzigen dies nur teilweise. So sind in Sachsen und Rheinland-Pfalz nur abgeschwächte Befugnisse der Datenschutzbeauftragten vorgesehen. Die Befugnis des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, nach § 42 Abs. 2 LDSG RP Anordnungen zu treffen, ist auf *erhebliche* Datenschutzverstöße beschränkt. Eine vergleichbare Regelung enthält § 40 SächsDSUG-E. Das Erfordernis eines erheblichen Verstoßes schränkt die Handlungsmöglichkeiten der Datenschutzaufsicht jedoch stark ein, denn es ist unklar, ab welcher Schwelle ein gravierender Verstoß vorliegt. Es leuchtet auch nicht ein, gewisse Verstöße als „Kavaliersdelikte“ jeder Sanktionsmöglichkeit durch die Aufsicht zu entziehen.

Noch weiter eingeschränkt sind die Befugnisse der Aufsicht in den Regelungen von Hessen (§ 14 Abs. 3 HDSIG), Thüringen (§ 7 Abs. 6 ThürDSAnpUG-EU) und Berlin (§ 13 Abs. 2 BlnDSG). Nach § 7 Abs. 6 Satz 1 ThürDSAnpUG-EU hat der LfDI Thüringen bei Verstößen zunächst eine Beanstandung auszusprechen und eine Stellungnahme des Verantwortlichen einzuholen. Nach Satz 5 der Vorschrift kann er erst weitere Maßnahmen von der obersten Landesbehörde und der Aufsichtsbehörde einfordern (aber nicht selbst treffen), wenn der Verstoß nach der Beanstandung nicht behoben wird. Eine ähnliche Regelung findet sich in § 13 Abs. 2 BlnDSG.

Die Beanstandung selbst hat keine Sanktionswirkung und führt lediglich dazu, dass der Adressat dazu verpflichtet wird, sich mit ihrem Gegenstand zu befassen. Eine wirksame Einwirkungsmöglichkeit im Sinne von Art. 47 Abs. 2 JIRL fehlt demnach. Die Datenschutzaufsicht bleibt damit im polizeilichen Bereich in mehreren Ländern zahnlos. Dabei zeigt die Erfahrung, dass es auch bei der Polizei zu mitunter ernsthaften Datenschutzverstößen kommt. Ein aktuelles Beispiel dafür sind die Drohbriefe an die Rechtsanwältin Seda Ba#ay-Y#ld#z, deren persönliche

Daten aus einer Polizeidatenbank abgerufen wurden. Nach Angaben der Berliner Datenschutzbeauftragten Maja Smoltczyk habe es auch in Berlin Drohbriefe an Privatpersonen gegeben, deren Daten „augenscheinlich von Polizei oder Justiz gestammt hätten“. Eine unabhängige Aufsicht mit wirksamen Befugnissen könnte helfen, solche und andere Datenschutzverstöße einzudämmen.

Fazit: Bedarf zur Nachbesserung

Die Umsetzungen der JIRL im polizeilichen Bereich weisen einige strukturelle Regelungsfehler auf. Diese betreffen zentrale Themen wie die Tauglichkeit der Einwilligung als Grundlage von Datenverarbeitungen, die Betroffenenrechte und die Aufsichtsbefugnisse der Landesdatenschutzbeauftragten. Diese Aspekte haben mehrere Landesgesetzgeber fehlerhaft umgesetzt bzw. sind dabei, dies zu tun. Auch angesichts der Risiken und Missbrauchspotentiale, die mit den immensen polizeilichen Datenbeständen verbunden sind, verdient dieser Regelungsbereich eine größere Aufmerksamkeit und sorgfältigere Regelungen. Der polizeiliche Datenschutz darf im Schatten von DSGVO und anderweitigen Polizeirechtsreformen nicht vernachlässigt werden. Es ist zu hoffen, dass in den noch laufenden Gesetzgebungsverfahren sowie in Ergänzung der abgeschlossenen Verfahren Nachbesserungen erfolgen.

Zitiervorschlag: Golla/Michel, Baustellen im polizeilichen Datenschutz – Zur Umsetzung der JIRL in den Ländern, JuWissBlog Nr. 42/2019 v. 19.3.2019, https://www.juwiss.de/42-2019/